ANNUAL 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017.

1. Date filed: March 1, 2018

2. Name of company(s) covered by this certification: BARConnects, LLC

3. Form 499 Filer ID: 143048254

4. Name of signatory: Michael Keyser

5. Title of signatory: Chief Executive Officer, BARC Electric Cooperative (parent)

6. Certification:

I, Michael Keyser, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company **has not** taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company **has not** received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed:

Attachments: Accompanying Statement explaining CPNI procedures

Summary of CPNI Compliance Policies of
BARConnects, LLC

The following summary describes the policies of BARConnects, LLC ("BARConnects"). These policies are designed to protect the confidentiality of CPNI and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. § 2001, *et seq*. These policies are administered by BARConnects General Manager, Gary Sickler, hereinafter referred to as the CPNI Compliance Manager.

BARConnects's policy, administered by its CPNI Compliance Manager, establishes the following policies regarding the use and disclosure of CPNI:

1. USE, DISCLOSURE OF, AND ACCESS TO CPNI

BARConnects will use, disclose, or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service; to initiate, render, bill and collect for communications services; to protect the rights or property of BARConnects, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law (such as pursuant to a valid request from law enforcement or a court order or other appropriate authority); or as expressly authorized by the customer.

BARConnects does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. It is BARConnects's current policy not to use CPNI for marketing. BARConnects does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. When BARConnects receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

2. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, BARConnects will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to BARConnects's existing policies that would strengthen protection of CPNI, they should report such information immediately to BARConnects's CPNI Compliance Manager so that BARConnects may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to BARConnects Requesting CPNI

BARConnects will not disclose any CPNI to an inbound caller until the caller's identity has been reasonably authenticated. BARConnects does not disclose Call Detail Information (CDI) to inbound callers. CDI includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or

duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. CDI may be provided by calling the customer at their telephone number of record or sending the information to the customer's address of record.

B. In-Person Disclosure of CPNI at BARConnects Offices

BARConnects may disclose a customer's CPNI to an authorized person visiting a BARConnects office upon verifying through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) that the person is authorized to receive such information.

C. Online Accounts

BARConnects does not provide access to account information online.

D. Notice of Account Changes

If and when an address of record is created or changed, BARConnects will send a notice to customer's preexisting address of record notifying them of the change. This notification is not required when the customer initiates service. The notice will not reveal the changed information and will direct the customer to notify BARConnects immediately if they did not authorize the change.

E. Business Customer Exemption

The authentication requirements for disclosure of CPNI do not apply to disclosure of business customer information by a dedicated account representative who knows through personal experience that the person requesting the information is authorized representative of the customer and that the contract between BARConnects and that business customer specifically addresses the protection of CPNI.

3. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any BARConnects employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to BARConnects's CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is BARConnects's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate BARConnects's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a BARConnects employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to BARConnects's CPNI Compliance Manager, who will determine whether to report the incident to law enforcement and/or take other appropriate action. BARConnects's Compliance Manager will determine whether it is appropriate to update BARConnects's CPNI policies or training materials in light of any new information; the FCC's rules require BARConnects on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, BARConnects's CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. Company's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions.

BARConnects will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below. A full business day does not count a business day on which the notice was provided. Federal law requires compliance with this requirement even if state law requires disclosure.

If BARConnects receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

BARConnects will delay notification to customers or the public upon request of the FBI or USSS. If BARConnects believes there is a need to disclose a breach sooner, the CPNI Compliance Manager should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; BARConnects still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

4. RECORD RETENTION

The CPNI Compliance Manager is responsible for assuring that BARConnects maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

BARConnects maintains a record, for a period of at least one year, of: those limited circumstances in which CPNI is disclosed or where third parties were allowed access to CPNI (i.e., pursuant to a valid request from law enforcement, court order or other appropriate authority); of supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI; its sales and marketing campaigns that use its customers' CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services offered as a part of the campaign; and records associated with customers' approval or nonapproval to use CPNI, and of notification to customers prior to any solicitation for customer approval of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

BARConnects maintains a record of all customer complaints related to its handling of CPNI, and records of BARConnects's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that BARConnects considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

BARConnects will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that BARConnects has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how BARConnects's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

5. TRAINING

All BARConnects employees with access to CPNI receive training and a copy of BARConnects's CPNI policies. The training includes emphasis that violations of its CPNI policies will result in disciplinary action, including the termination of employment where appropriate, and also that employees may be subject to criminal penalties if they knowingly facilitate the unauthorized disclosure of a customer's confidential information.